Wired for Management Compliance Test Plan

Compliance Test Plan for Wired for Management Version 1.1 Client Systems

August 7, 1997
Intel Corporation

CONTENTS

Section
1

Introduction

Wired for Management Compliance

This document provides a comprehensive set of tests for Network and Managed PC platforms that desire to be compliant with the Wired for Management Version 1.1 specification. Any client platform that passes all of the tests contained in this document can be considered compliant to this specification. Wired for Management compliance, as used in this document, means that all of the management features required by the Wired for Management Version 1.1 Baseline are present and functional .

Compliance Test Approach

Client systems will be placed in several different configurations of a Compliance Test Network. The configuration of the test network will be defined by the specific test. Tests will then be executed on the client to provide coverage for all of the manageability features contained in the Wired for Management Baseline 1.1 specification.

Revision History

Date	Author	Revision
8/4/97	Stan Booher	1st Draft

Relevant Documents

- **Wired for Management Baseline 1.1 Specification**
- **DMTF DMI v2.0 Specification**
- **PXE Test Design Specification**

Section
2

Wired for Management Overview

Wired for Management Initiative

Wired for Management (WfM) is an Intel initiative to improve the manageability of desktop, mobile, and server systems. The goal of WfM is to reduce the Total Cost of Ownership (TCO) through improved manageability. The Wired for Management Baseline addresses improved manageability in four technology areas:

- Remote New System Setup
- Remote Wake-Up
- Instrumentation
- Power Management

Manageability features in each of these four technology areas combine to form the Wired for Management Baseline Specification.

Remote New System Setup

The WfM Baseline specifies the protocols by which a client requests and downloads an executable image from a server and the minimum requirements on the client execution environment when the downloaded image is executed. It does not specify the implementation details of preboot code on the client or the provisions for security (authorization, privacy, and data integrity) during the exchanges between the client and the server. The WfM Baseline requires a compliant PC to be capable of using DHCP and TFTP as described (in Appendix A of the WfM specification) to effect the installation of an OS from a server. The conditions under which the PC initiates remote OS installation are implementation dependent.

Remote Wake-Up

If a PC supports a reduced power state, it must be possible to bring the system to a fully powered state in which all management interfaces are available. Typically, the LAN adapter recognizes a special packet as a signal to wake up the system. Remote wakeup can also be accomplished by rebooting the system from its low-power state. For hardware implementations that don't support a transition from the system's current low-power state to its full-power state while preserving context, rebooting is the only viable solution.

Instrumentation

The WfM Baseline requires that compliant platforms utilize the DMI v2.00 Management Interface (MI) and Component Interface (CI) application programming interfaces and host a

DMI v2.00 Service Provider, as defined by the DMTF. This Baseline Instrumentation specification also identifies specific DMI standard groups, including event generation groups, that must be instrumented for a Baseline-compliant platform.

Power Management

WfM Baseline compliant systems have four distinct power states: Working, Sleeping, Soft Off, and Mechanical Off. In the Working state, user mode application threads are dispatched and running. Individual devices and processors may be in low-power states if they are not being used. When the computer is idle or the user has pressed the power button, the OS will put the computer into one of the sleeping states (Sleep or Soft Off). No user-visible computation occurs in a sleeping state. The sleeping states differ in what events can bring the system to a Working state, and how long this takes. For example pressing a key will cause a wake-up from the Sleeping state whereas a Remote Wake-up event or power switch is needed to wake from the Soft Off state.

Section
3

Compliance Test Network

Test Network Environment

Network Hardware Requirements

Test environment hardware consists of hubs and routers as shown in figure 1.0 WfM Compliance Test Network. All network components must be capable of supporting 100Mb communications. Management services will be provided by an LCM 1.5 and a separate server will provide DHCP services (as well as BootP services for certain tests). A PC asset will be placed on the network to act as a platform for tools required by some tests. Some tests require the presence of other Network or Managed PC clients. Therefore, 3 Intel Network PCs will be placed on the network to support these tests. The Compliance Test network along with the LCM 1.5, DMI Test PC, and the 3 Intel Network PCs will considered a reference network system.

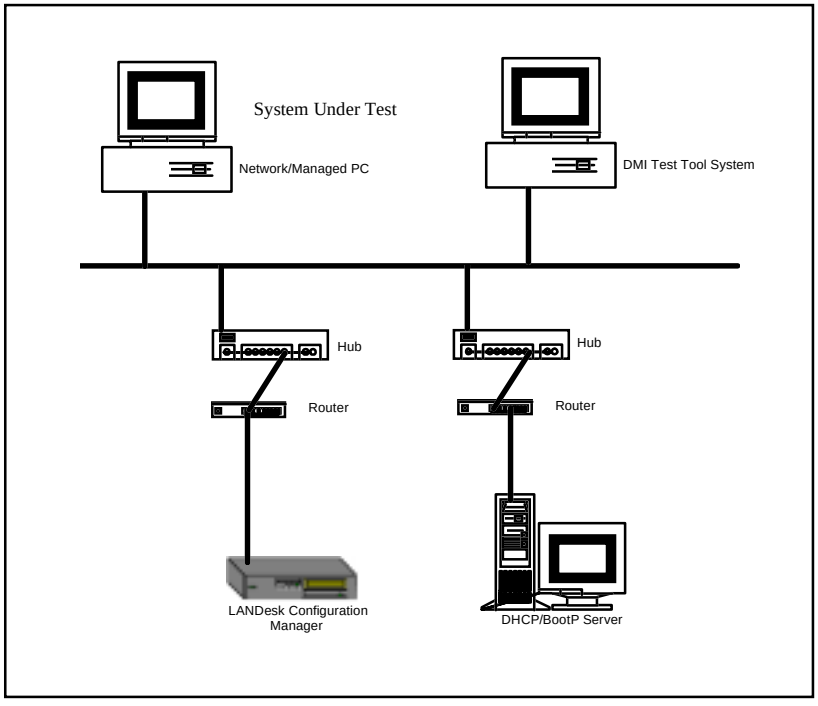

Fig. 1.0 WfM Compliance Test Network

Network Software Requirements

Test environment software consists of manageability software capable of supporting the tests described in this document. Supported functions include remote setup of new system, transmission of a Wake-Up packet, and DMI test routines.

Test Network Configurations

Hardware and software requirements in support of the compliance test cases are shown below. Each of the compliance test cases will refer to one or more of the hardware/software configurations.

Hardware Configuration Matrix			
Config ID	**Server/Wksta**	**OS Requirements**	**Software Requirements**
CFG01	Non LCM DHCP Server	NT Server 4.0	DHCP Server
CFG02	BOOTP Server	NT Server 4.0	TFTP enabled
CFG04	LCM as Proxy DHCP	NT Server 4.0	BINL and TFTP enabled
CFG05	PC as DMI test Platform	NT Workstation 4.0	Compchk test tool

Section
4

Compliance Test Descriptions

Remote New System Setup

DHCP Tests

The DHCP Preference Regressions Test Cases exercise proper distribution and receipt of leased IP addresses and switch to Bootp in absence of a Configuration Management server. Execution of some of these test cases will require several other Network or Managed PC clients to be present on the network one of which will be the client system under test.

Case ID	Test Case	Expected Result
DHCP.100	On a single subnet, set up CFG02. BOOTP needs to be configured to download BSTRAP.1 Perform a Service Boot on a client.	Client should receive IP address and boot filename from server. Execution of boot file will produce error stating "PXE-E72: "PXEClient" class option not found." This signifies successful download and execution of boot file. If this error recd, pass.
DHCP.107	Set up CFG01 with a valid scope on a separate subnet than an PXE client, separated by two routers. Perform a Service Boot on the client.	DHCP should issue a valid IP address to the client and allow for connection to the network.
DHCP.108	Set up CFG01 with a valid scope of 3 addresses on a separate subnet than 4 PXE clients, separated by two routers. Perform a Service Boot on the clients.	DHCP should issue a valid IP address to only 3 clients and display an error to the 4th.
DHCP.109	Set up CFG01with a valid scope of 3 addresses. Configure 4 clients on a separate subnet than the server; 3 as DHCP clients and one having a static IP address that matches a number in the server scope. Perform a Service Boot on all six clients.	An IP address conflict message should be displayed to the DHCP client with the conflicting address.

Proxy Tests

The Proxy Procedure Regressions Test Cases exercise proper receipt of DHCP offers from the DHCP server (with IP address) and from the LCM proxy (with null IP address).

Case ID	Test Case	Expected Result
PROX.101	Set up CFG01 and CFG04 on one subnet. Perform a Service Boot from a client on a second subnet separated by two routers.	Client should receive an IP address from the DHCP server and a null address from the Proxy.

Case ID	Test Case	Expected Result
PROX.104	Set up CFG01 on one subnet, CFG04 on a second subnet and a client on a third subnet. Perform a Service Boot.	Client should receive an IP address from the DHCP server and a null address from the Proxy.

TFTP/MTFTP Tests

The TFTP - MTFTP Regression Test Cases exercise client master/slave negotiations as part of MTFTP and MTFTP time out handling. Execution of some of these test cases will require several other Network or Managed PC clients to be present on the network one of which will be the client system under test.

Case ID	Test Case	Expected Result
TFTP.100	Set up CFG01 and CFG04 on a single subnet. Perform a Service Boot on 4 clients.	One client will negotiate to become Master client while all others capture packets as Slaves. All clients will eventually receive all packets and perform a service boot. Master client is signified by ~ symbol during MTFTP and Slaves by ~ during MTFTP.
TFTP.102	Set up CFG01 and CFG04 on a single subnet. Perform a Service Boot on 4 clients, 2 on the same subnet as the servers and 2 on a second subnet separating them from the servers by at least two routers.	One client will negotiate to become Master client while all others capture packets as Slaves. All clients will eventually receive all packets and perform a service boot. Master client is signified by ~ symbol during MTFTP and Slaves by ~ during MTFTP.
TFTP.103	Set up CFG01 and CFG04 on a single subnet. Perform a Service Boot on 4 clients, 2 on the same subnet as the servers and 2 on a second subnet separating them from the servers by at least two routers. Disable Multicast routing on one router.	Clients on the same subnet as the servers will receive the packets via multicast, signified by the ~ symbol during MTFTP. The clients on the second subnet will time-out on MTFTP and receive the packets via Unicast. This signified by time-out to TFTP.

PXE API Tests

API testing will be executed as described in the PXE Test Plan. Specifically, the PXE API test will be installed in a test LCM. On boot up the PXE test will be selected and executed. The results from the API test will be reviewed, an failures noted.

Case ID	Test Case	Expected Result
API.100	Set up CFG01, CFG04, and the client on one subnet. Perform a Service Boot on the client and perform the selections necessary to load and run the PXE API test.	The client should complete the API test and write results to a file on the virtual a: drive. Review the file to ensure no errors were encountered.

Remote New System Setup Functional Tests

This test will ensure that an entire management service can be performed by a client system. The management service used in this test will exercise all of the service categories provided by the LCM 1.5 management server used in the reference network. The intent of this is to provide an end-to-end test of a remote new system setup exchange between the client and the server.

Case ID	Test Case	Expected Result
FUN.100	Set up CFG01 on one subnet, CFG04 on a second subnet, and the client on a third subnet. Perform a Service Boot on the client. Service will include full disk format, OS install of NT 4.0 Server, application install of Windows 97.	The client should complete the entire new system set-up service.

Remote Wake-Up

These tests will validate the client Remote Wake-Up support. The tests cover three conditions; valid wake-up packet, wake-up packet with a single bit error, and valid non-wake up packet.

Case ID	Test Case	Expected Result
RWU.100	Set up CFG01 and CFG04 on a single subnet. Set up the client on the same subnet. Place the client in a soft-off state. Send the client a properly formatted wake-up packet.	The client should recognize the wake-up packet and transition to the working state.
RWU.101	Set up CFG01 and CFG04 on a single subnet. Set up the client on the same subnet. Place the client in a soft-off state. Send the client a wake-up packet with single bit error in the address portion of the message body.	The client should remain in the soft-off state.
RWU.102	Set up CFG01 and CFG04 on a single subnet. Set up the client on the same subnet. Place the client in a soft-off state. Send the client a properly formatted non-wake-up packet.	The client should remain in the oft of state.

Instrumentation

Instrumentation compliance is tested via the DMI compchk test tool.

Case ID	Test Case	Expected Result
INS.100	Setup CFG01 and CFG05 on a single subnet. Setup the client on the same subnet. Using the compchk tool, connect to the client using RPC.	RPC connection should complete successfully and the client MIFs should be visible in the compchk window.
INS.101	Setup CFG01 and CFG05 on a single subnet. Setup the client on the same subnet. Using the compchk tool, connect to the client using RPC. Select the master mif file for the DMI 2.0 portion of the test, and the wfm file for the required portion of the test. Execute the compchk test.	RPC connection should complete successfully and the client MIFs should be visible in the compchk window. Client mifs should successfully pass both the master and WfM portions of the test.

Power Management

Power management compliance is tested by exercising transitions between the Wired for Management required power states.

Case ID	Test Case	Expected Result
POW.100	Setup the client and launch any application to place the system in working state. Leave the system idle and allow the system to enter sleep state. Press a keyboard key to begin transition to working state.	System should transition from sleep state to working state.
POW.101	From the working state execute a shutdown of the client system. Press the soft on/off switch	System should transition from soft off state to working state. System should boot to the installed OS.
POW.102	From the working state execute a shutdown of the client system. Send the client system a valid wake-up packet.	System should transition from soft off state to working state. System should boot to the installed OS.
POW.103	From the working state execute a shutdown of the client system. Locate the mechanical on/off switch and place it in off position. Toggle the soft on/off switch.	System should transition to and remain in mechanical off state.

Wired for Management 1.1 Compliance Checklist for Client Platforms

Case ID	Results	Comments
DHCP.100	PASS ❑ FAIL ❑	
DHCP.107	PASS ❑ FAIL ❑	
DHCP.108	PASS ❑ FAIL ❑	
DHCP.109	PASS ❑ FAIL ❑	
PROX.101	PASS ❑ FAIL ❑	
PROX.104	PASS ❑ FAIL ❑	
TFTP.100	PASS ❑ FAIL ❑	
TFTP.102	PASS ❑ FAIL ❑	
TFTP.103	PASS ❑ FAIL ❑	
API.100	PASS ❑ FAIL ❑	
FUN.100	PASS ❑ FAIL ❑	
RWU.100	PASS ❑ FAIL ❑	
RWU.101	PASS ❑ FAIL ❑	
RWU.102	PASS ❑ FAIL ❑	
INS.100	PASS ❑ FAIL ❑	
INS.101	PASS ❑ FAIL ❑	

Case ID	Results	Comments
POW.100	PASS ❑ FAIL ❑	
POW.101	PASS ❑ FAIL ❑	
POW.102	PASS ❑ FAIL ❑	
POW.103	PASS ❑ FAIL ❑	